

DETAILED ACTION

1. Claims 1-7, 14-20, 25-31, 36 and 39-44 are pending in this application.

Examiner's Amendment

An Examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to the Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephonic interview and in an electronic mail by Ryan P. Wallace and Martin M. Zoltick on 04/20/2009.

The application has been amended as follows:

1. (Currently Amended) A system, comprising:
 - a deterministic network;
 - a computer executing a hard real-time operating system, said computer being connected to the deterministic network;
 - an application running under the hard real-time operating system;
 - a security process running under the hard real-time operating system; and
 - an external monitor connected to the deterministic network, wherein the security process is configured to periodically, in hard real-time, check the integrity of the application and/or a data element used by the application and, if the integrity check of the application or the data element indicates that the application or

data element has been tampered with, notify a user of the system and/or shut down at least part of the system or application, and

the security process includes a challenge handler that is configured to (i) receive a challenge transmitted from the external monitor to the challenge handler via the deterministic network and (ii) transmit to the external monitor via the deterministic network a response to the challenge within a specified hard real-time interval of less than five milliseconds from the challenge handler receiving the challenge, wherein the external monitor is configured so that if the external monitor does not receive the response within the specified hard real-time interval of five milliseconds or less from sending the challenge, the external monitor issues a notification and/or shuts down at least part of the system or application.

2. (Currently Amended) In a computer system running a real-time operating system, a computer security method, comprising:

executing a security process under the real-time operating system, wherein the security process is configured to periodically, in hard real-time, check the integrity of an application and/or a data element used by the application and issue a notification and/or shut down the application if the integrity check of the application or the data element indicates that the application or data element has been tampered with;

sending, from an external monitor, a challenge to the security process or to a challenge handler that monitors the integrity of the security process via a deterministic network;

sending to the external monitor via the deterministic network a response to the challenge, wherein the response is sent within a specified hard real-time interval of less than five milliseconds from when the challenge was received; and

issuing a notification and/or shutting down at least part of the computer system or the application if a response to the challenge is not received within the specified hard real-time interval of five milliseconds or less from when the challenge was sent.

3. (Currently Amended) A computer system, comprising:

a dual-kernel operating system comprising a hard_real-time kernel and a non-real-time kernel;

a first real-time thread running under the hard_real-time kernel, the first real-time thread being configured to monitor the integrity of an application running under the non-real-time kernel;

a second real-time thread running under the hard_real-time kernel, the second real-time thread being configured to monitor integrity of the first real-time thread;

a security process running under the non-real-time kernel, the security process being configured to check the integrity of the first real-time thread and the second real-time thread;

a challenge handler executing under the hard real-time kernel; and

an external monitor programmed to determine whether the response from the challenge handler was received by the external monitor within a specified hard real-time interval of less than five milliseconds from the challenge handler sending the challenge

and to raise an alarm if it determines that the response from the challenge handler was not received by the external monitor within the specified hard real-time interval of less than five milliseconds from the challenge handler sending the challenge.

Allowable Subject Matter

2. The following is an Examiner's statement of reasons for allowance: Claims 1-7, 14-20, 25-31, 36 and 39-44 are allowed.
3. The prior art of record doesn't teach or suggest or render obvious either alone/or in combination an external monitor programmed to determine whether a response from a challenge handler was received by the external monitor within a specified hard real-time interval of less than five milliseconds from the challenge handler sending the challenge and to raise an alarm if it determines that the response from the challenge handler was not received by the external monitor within the specified hard real-time interval of less than five milliseconds from the challenge handler sending the challenge.
4. Any comments considered necessary by the Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance or Examiner Amendment."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Suman Debnath
/S. D./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435